

CLAIMS

What is claimed is:

1. A method comprising:
generating a message digests on a client connected with a network wherein said message digests uniquely identify contents of files stored on the client;
synchronizing contents of said client with a repository connected with the network based on contents of the message digests on the client and corresponding entries in a database of message digests stored on the repository; and
verifying that the contents of the repository match the contents of the client.
2. The method of claim 1, further comprising storing the message digests on the client after generating the message digests.
3. The method of claim 2, further comprising generating new message digests for all files on the client to be cached on the repository prior to data synchronization.
4. The method of claim 1, wherein said files stored on the client comprise a subset of all files stored on the client.
5. The method of claim 4, wherein said subset comprises only files stored in specified directories.

6. The method of claim 1, wherein said generating message digests comprises generating a cryptographic hash for each file to be synchronized.
7. The method of claim 6, wherein said cryptographic hash comprises 128 to 160 bits.
8. The method of claim 1, wherein said synchronizing contents of said client with a repository comprises:
 - generating a first message digest for a file stored on the client;
 - reading a second message digest from the database of message digests from the repository corresponding to the first message digest;
 - comparing the first message digest to the second message digest;
 - determining whether contents of the client match contents of the repository based on said comparing the first message digest to the second message digest;
 - copying files from the client to the repository if the files are not found on the repository or do not match the files found on the repository; and
 - updating the database of message digests on the repository by copying the message digest from the client to the database on the repository.
9. The method of claim 1, wherein said verifying that the contents of the repository match the contents of the client comprises:
 - generating a first cryptographic hash from a list of message digests for all files on the client to be cached on the repository;
 - generating a second cryptographic hash from the contents of the database of message digests from the repository;
 - comparing the first and second cryptographic hash; and

repeating client and repository synchronization if the first and second cryptographic hashes do not match.

10. A system comprising:
a repository server connected with a network, to function as a data repository on behalf of a client; and
the client connected with said repository server via the network, wherein said client
generates a plurality of message digests that each uniquely identify the content of a
corresponding file stored on the client,
synchronizes contents of said client with files stored in the repository server based on
contents of the message digests on the client and a database of message
digests stored on the repository, and
verifies whether the contents of the repository match the contents of the client.
11. The system of claim 10, wherein said generating a plurality of message digests comprises performing a cryptographic hash for each file to be synchronized.
12. The system of claim 11, wherein said cryptographic hash comprises 128 to 160 bits.
13. The system of claim 10, wherein said client:
reads a first message digest generated on the client;
reads a second message digest from the database of message digests from the repository
corresponding to the first message digest;
compares the first message digest to the second message digest;

determines whether contents of the client match contents of the repository based on said
comparing the first message digest to the second message digest;
copies files from the client to the repository if the files are not found on the repository or do
not match the files found on the repository; and
updates the database of message digests on the repository by copying the message digest
from the client to the database on the repository.

14. The system of claim 10, wherein said client:
generates a first cryptographic hash from the message digest on the client;
generates a second cryptographic hash from the database of message digests from the
repository;
compares the first and second cryptographic hash; and
repeats client and repository synchronization if the first and second cryptographic hashes do
not match.
15. A system comprising:
a client connected with a repository server via a network, wherein said client generates a
plurality of message digests that each uniquely identify the content of a corresponding
file stored on the client; and
the repository server connected with the network, to function as a data repository on behalf of
the client, wherein said repository server
synchronizes contents of said client with files stored in the repository server based on
contents of the message digests on the client and a database of message
digests stored on the repository, and
verifies whether the contents of the repository match the contents of the client.

16. The system of claim 15, wherein said generating a plurality of message digests comprises performing a cryptographic hash for each file to be synchronized.
17. The system of claim 16, wherein said cryptographic hash comprises 128 to 160 bits.
18. The system of claim 15, wherein said repository server:
reads a first message digest generated on the client;
reads a second message digest from the database of message digests from the repository
corresponding to the first message digest;
compares the first message digest to the second message digest;
determines whether contents of the client match contents of the repository based on said
comparing the first message digest to the second message digest;
copies files from the client to the repository if the files are not found on the repository or do
not match the files found on the repository; and
updates the database of message digests on the repository by copying the message digest
from the client to the database on the repository.
19. The system of claim 15, wherein said repository server:
generates a first cryptographic hash from the message digest on the client;
generates a second cryptographic hash from the database of message digests from the
repository;
compares the first and second cryptographic hash; and
repeats client and repository synchronization if the first and second cryptographic hashes do
not match.

20. A machine-readable medium having stored thereon data representing sequences of instructions, said sequences of instructions which, when executed by a processor, cause said processor to:
 - generate message digests on a client connected with a network wherein said message digests uniquely identify contents of files stored on the client;
 - synchronize contents of said client with a repository connected with the network based on contents of the message digests on the client and corresponding entries in a database of message digests stored on the repository; and
 - verify that the contents of the repository match the contents of the client.
21. The machine-readable medium of claim 20, wherein said client stores the message digests on the client after generating the message digests.
22. The machine-readable medium of claim 21, wherein said client generates new message digests for all files on the client to be cached on the repository prior to data synchronization.
23. The machine-readable medium of claim 20, wherein said files stored on the client comprise a subset of all files stored on the client.
24. The machine-readable medium of claim 23, wherein said subset comprises only files stored in specified directories.
25. The machine-readable medium of claim 20, wherein said client generates a cryptographic hash for each file to be synchronized;

096634 062004
T06290 T2E95850

26. The machine-readable medium of claim 25, wherein said cryptographic hash comprises 128 to 160 bits.
27. The machine-readable medium of claim 20, wherein said client:
 - generates a first message digest for a file stored on the client;
 - reads a second message digest from the database of message digests from the repository
 - corresponding to the first message digest;
 - compares the first message digest to the second message digest;
 - determines whether contents of the client match contents of the repository;
 - copies files from the client to the repository if the files are not found on the repository or do
 - not match the files found on the repository; and
 - updates the database of message digests on the repository by copying the message digest
 - from the client to the database on the repository.
28. The machine-readable medium of claim 20, wherein said client:
 - generates a first cryptographic hash from a list of message digests for all files on the client to
 - be cached on the repository;
 - generates a second cryptographic hash from the contents of the database of message digests
 - from the repository;
 - compares the first and second cryptographic hash; and
 - repeats client and repository synchronization if the first and second cryptographic hashes do
 - not match.